



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884**

April 5, 2001

INSPECTOR GENERAL INSTRUCTION 7950.3

SUBJECT: Mobile Computing Devices

References: See Appendix A.

A. Purpose. This Instruction establishes the Office of the Inspector General, Department of Defense (OIG, DoD), Mobile Computing Device policy.

B. Applicability and Scope

1. This Instruction applies to the Offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; Director, Intelligence Review; and the Office of the Deputy General Counsel (Inspector General), which is provided support by the OIG, DoD, when its Office of the Secretary of Defense-provided equipment interfaces with the OIG, DoD, network. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

2. This Instruction applies to all mobile computing devices, whether Government-issued or personally owned.

C. Definitions. See Appendix B.

D. Background

1. Mobile computing devices may include features such as infrared, radio frequency, and telephone modem communications capabilities. These same features allow easy connectivity between a mobile computing device and other devices for performing data exchanges and along with their expanded memory and processing ability, create new vulnerabilities for compromise. Attempts to temporarily disable these features by external means may not actually be solutions and, in some cases, may even enhance the associated vulnerabilities. The transmission of information between a wireless device and an Internet server is no different than a radio broadcast. Anyone with a receiver can eavesdrop. Wireless messages can be intercepted or tampered with in ways not possible with wired connections.

2. Since most, if not all, units are capable of both sending and receiving without indication to the user, this feature poses a high security risk.

3. When mobile computing devices are permitted within the OIG, DoD, an enormous amount of trust is placed on the user to provide physical security for the device. Contained within the mobile computing device are all the components needed for a remotely activated surveillance device.

E. Policy

Report Documentation Page

Report Date 05 Apr 2001	Report Type N/A	Dates Covered (from... to) - -
Title and Subtitle Mobile Computing Devices		Contract Number
		Grant Number
		Program Element Number
Author(s)		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884		Performing Organization Report Number
Sponsoring/Monitoring Agency Name(s) and Address(es)		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified		Classification of this page unclassified
Classification of Abstract unclassified		Limitation of Abstract UU
Number of Pages 6		

1. Mobile computing devices are not standard hardware or software, as specified in reference a.
2. The OIG, DoD, shall not compromise sensitive data, as defined in references b, c, and d via mobile computing devices, which may be referred to as personal digital assistants, palm tops, hand-held computers and workstations, web based enhanced cell phones, two-way pagers, and wireless E-mail devices. Classified data processing shall be performed only on accredited, classified systems.
3. In accordance with reference e, mobile computing devices shall not be used in areas where classified material is processed or discussed.
4. Users should not attempt to block sending and receiving features using any method that has not been approved by the Designated Approving Authority (DAA). The DAA is the official designated by the Inspector General, DoD, who has the authority to decide on accepting the security safeguards prescribed for an information system. The DAA is currently the Director, Administration and Information Management (OA&IM).
5. Since these devices may be used as a tool for managing tasks, calendars, and staying in virtual constant contact with the OIG, DoD, an increased potential exists for compromise of sensitive data. It is the responsibility of employees to ensure that their use of such devices does not lead to loss or exposure of information.
6. Appropriate physical security guidelines and procedures, as discussed in reference b, are of paramount importance. The risk of compromising classified or sensitive information, resulting from users losing their mobile computing devices, is considered high by reference e. If an adversary gained access to the mobile computing device for as little as 30 minutes, it could be reconfigured to collect, process, store, and retransmit classified or sensitive data from within the secure space, according to reference e. Users are also strongly cautioned to protect their mobile computing devices during transit and report any suspicious activity involving their devices to the Personnel and Security Directorate, OA&IM.
7. Mobile computing devices shall not be taken into any Sensitive Compartmented Information Facility (SCIF), a Special Access Program (SAP) facility, or a Special Access Required (SAR) facility.
8. Mobile computing devices can transmit computer viruses if their contents are uploaded to OIG, DoD, computers. Therefore, software that permits uploading will be loaded on OIG, DoD, computers only on an exception basis.
9. E-mail messages, like all electronic documents, may be considered agency records and are subject to the provisions of references f, g, and h.
10. Users may not use unofficial E-mail services for official business without the express permission of the Information Systems Directorate, OA&IM.
11. Failure to adhere to the provisions of this Instruction may result in termination of access to all OIG, DoD-supported local area networks and in other disciplinary and legal penalties, as appropriate.
12. Government-owned mobile computing devices shall be procured in accordance with reference i.
13. Only OIG, DoD-procured third party Internet services subscriptions will be permitted on Government mobile computing devices.

F. **Responsibilities**

1. The **Inspector General, DoD**, shall designate the DAA.

2. The **DAA** shall decide on accepting the security safeguards prescribed for mobile computing devices.

3. The **OIG Component Heads** shall ensure that the provisions of this Instruction and references a through i are implemented.

4. The **Personnel and Security Directorate, OA&IM**, shall advise and assist management on appropriate administrative action if misuse occurs.

5. The **Information Systems Directorate, OA&IM**, shall load software to enable uploading of information from mobile security devices only on an exception basis.

6. The **Administration and Logistics Services Directorate, OA&IM**, shall assist and advise when E-mail messages constitute records subject to the provisions of references f, g, and h.

7. **End Users** shall:

a. Not use mobile computing devices in areas where classified material is processed or discussed.

b. Not take mobile computing devices into a SCIF or SAP/SAR facilities.

c. Keep in mind that E-mail is subject to the provisions of references f, g, and h.

d. Not use unofficial E-mail services for official business without the express permission of the Information Systems Directorate, OA&IM.

e. Not upload information stored on a mobile computing device into the OIG, DoD, environment without the express permission of the Information Systems Directorate, OA&IM.

f. Refrain from any practices that might jeopardize, compromise, or render useless any OIG, DoD, data, system or network.

g. Be individually responsible and liable for any disclosures of sensitive information if the employee sends such information through a mobile computing device.

h. Not send secure, sensitive, classified, or potentially compromising information through a mobile computing device unless approved by the DAA. All classified data transfers shall be performed only on accredited, classified systems. Information subject to references g and h shall be appropriately protected if transmitted electronically.

i. Maintain physical security of mobile computing devices at all times.

j. Not access the Internet or E-mail through the mobile computing device while it is connected to the computer (e.g. the device is in a cradle from which a cable runs to the microcomputer.) This provision applies even if software to enable uploading of information from mobile computing devices has been loaded by the Information Systems Directorate, OA&IM, on an exception basis.

G. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:



Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

**APPENDIX A
REFERENCES**

- a. IGDINST 7950.2, *Microcomputer Hardware and Software Management Program*, February 9, 2001.
- b. IGDINST 5200.40, *Security Requirements for Automated Information Systems*, July 20, 2000.
- c. DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AISs),” March 21, 1988.
- d. DoD 5200.28-M, “ADP Security Manual,” January 1973.
- e. National Security Agency Advisory IAA-001-01, “Personal Electronic Devices Security Guidance,” January 16, 2001.
- f. IGDM 5015.2, *Records Management Program*, June 2000.
- g. DoD Directive 5400.7, “DoD FOIA Program,” September 29, 1997.
- h. DoD 5400.11-R, “DoD Privacy Program,” August 1983.
- i. IGDINST 7950.1, *Acquisition of Information Technology Resources*, May 23, 2000.

APPENDIX B DEFINITIONS

- a. **Designated Approving Authority (DAA).** The official designated by the Inspector General, DoD, who has the authority to decide on accepting the security safeguards prescribed for an information system. The DAA issues an accreditation statement that records the decision to accept those standards. The DAA is currently the Director, OA&IM.
- b. **Electronic Mail (E-Mail).** A means of communication that uses computer-to-computer data transfer technology, normally as textual messages or attached files.
- c. **End-User.** An OIG, DoD, employee or contractor who uses automated equipment to perform work-related tasks.
- d. **Mobile Computing Device.** Electronics that have self-contained processing units, contain wireless telecommunications capabilities and are easily transportable. The definition includes, but is not limited to, equipment that may be referred to as personal digital assistants, palm tops, hand-held computers and workstations, web based enhanced cell phones, two-way pagers, and wireless E-mail devices
- e. **OIG Environment.** Any computer, media, or network used by the OIG, DoD.